

TED4363
ORIGIN DS-00

INFO	LOG-00	MFA-00	EEB-00	AF-00	AIT-00	A-00	CIAE-00
	INL-00	DNI-00	DODE-00	DOTE-00	WHA-00	PERC-00	EAP-00
	DHSE-00	EUR-00	OIGO-00	FAAE-00	OBO-00	TEDE-00	INR-00
	IO-00	CAC-00	MOFM-00	MOF-00	NEA-00	DCP-00	ISN-00
	NSCE-00	OIG-00	OMB-00	PA-00	PM-00	PPT-00	P-00
	ISNE-00	DOHS-00	FMPC-00	SP-00	IRM-00	SSO-00	SS-00
	DPM-00	USSS-00	NCTC-00	CBP-00	BBG-00	R-00	SCRS-00
	PMB-00	DSCC-00	SCA-00	SAS-00	FA-00	/000R	

P 311732Z MAR 09
FM SECSTATE WASHDC
TO SECURITY OFFICER COLLECTIVE PRIORITY
AMEMBASSY TRIPOLI PRIORITY
INFO AMCONSUL CASABLANCA PRIORITY
XMT AMCONSUL JOHANNESBURG
AMCONSUL JOHANNESBURG

S E C R E T STATE 030838

NOFORN

E.O. 12958: DECL: MR
TAGS: [ASEC](#)
SUBJECT: DIPLOMATIC SECURITY DAILY

Classified By: Derived from Multiple Sources

SECRET//FGI//NOFORN//MR

Declassify on: Source marked 25X1-human, Date of source:
March 30, 2009

1. (U) Diplomatic Security Daily, March 31, 2009
2. (U) 2009 NATO Summit - Paragraphs 8-16
3. (U) Significant Events - Paragraphs 17-23
4. (U) Key Concerns - Paragraphs 24-44
5. (U) Threats & Analysis - Paragraphs 45-59
6. (U) Cyber Threats - Paragraphs 60-68
7. (U) Suspicious Activity Incidents - Paragraphs 69-80
8. (U) 2009 NATO Summit
9. (SBU) DS/TIA/ITA is not in possession of any information that affects summit plans for the end of this week. Imminent threat information will be passed immediately.
10. (U) General vulnerabilities
11. (U) Police checkpoints: Stars & Stripes reported the following. "Germany and France have re-instituted border controls. Travelers should expect to be stopped and checked for proper identification as they cross borders. U.S. Citizens should be sure to carry their tourist passports to avoid hassles and possible fines for traveling without proper identification. Travelers on official duty may be authorized to enter France with official orders and identification. U.S. Army Europe officials recommend that all travelers consult with travel experts from their respective organizations about specific guidelines when traveling across any international border."
12. (SBU) DS/TIA/ITA has witnessed both German and French security checkpoint development over the weekend. Both nations have set up as-yet nominal checkpoints on either end of the Pont de l'Europe (Bridge of Europe, called Europabrücke in Kehl) vehicular bridge, causing minimal traffic backups; it is likely these checks and backups will increase as the week progresses. Police presence in

Strasbourg heightened as of Sunday morning, with barricades going up throughout the city and a noticeable contingent of gendarmes, who normally do not patrol urban areas, both on foot and on motorcycles. Police presence in Kehl has been increased, with the park at the German end of the Passerelle Bridge now off-limits for the remainder of the summit; the French side of the bridge is still open for pedestrians, but with heightened police presence. Preparations in Baden-Baden, as of Sunday afternoon, were less stringent, with noticeable police presence at the Oos Bahnhof (Baden-Baden's main train station), a likely demonstration site.

¶13. (U) Protest activity: Reuters reported, "Heinz From, head of Germany's domestic intelligence agency, told Reuters he saw 'a militant potential of some 3,000 people' at the Strasbourg protests."

¶14. (SBU) DS/TIA/ITA notes there has been no protest activity in Strasbourg; although, at least 5,000 were expected to demonstrate in the nearby university city of Freiburg, Germany, on Monday afternoon. Protests at the G-20 Summit in London have been peaceful to date; the chances of violent protest activity in Strasbourg will increase dramatically if violence occurs in London. The International Protest Camp, possibly host to at least 15,000 protesters beginning April 1, will be located south of Strasbourg in the village of La Ganzau. The camp, which is located 9 km south of the Passerelle photo opportunity site, 11 km south of the U.S. Consulate General, and 12 km south of RON and the Convention Center, is located on Rue de la Ganzau, a street that has been surveyed by Google.com's "Street View" program.

¶15. (U) Reuters also reported, "Police have evacuated Strasbourg University and will keep it closed for a week. Students protesting against the government's education policies had occupied the building, and university authorities feared anti-NATO demonstrators would join them; 13 schools will be closed along with sports fields."

¶16. (SBU) DS/TIA/ITA notes RON and the summit's main site at the Palais des Congrès (Convention Center) are located directly adjacent to a very large high school (Lyce Kleber), as well as the athletic fields for Strasbourg University. Although the university is closed, the high school remained open Monday, with a large influx of teenaged students around it at the beginning and end of the school day. Its closure on Friday will be integral to halting pedestrian traffic in the summit area in time for the Friday afternoon Town Hall meeting (U.S. President (POTUS) speaking, but Secretary of State (SecState) not attending) being held just north of the Convention Center. (Open sources)

¶17. (U) Significant Events

¶18. (SBU) EUR Turkey - Local Guard Force (LGF) Ankara identified three packages addressed to the POTUS, SecState, and U.S. Ambassador containing unknown white powder on March 30. Included in the packages were business cards for the director of an automotive plastics company. The LGF commander contacted the sender of the gifts, who explained he had sent a book and rock candy and that the contents must have been crushed in the mail. In light of the upcoming presidential visit, the RSO determined it was prudent to treat these packages as suspicious and handle them in accordance with established procedures. The suspicious powder was sent to the local Government of Turkey lab for analysis. (RSO Ankara Spot Report)

¶19. (C) AF Madagascar - Emergency Action Committee (EAC) Antananarivo convened March 27 to discuss the current state of affairs, the proposed weekend rallies, the status of security measures, and the need for additional tripwires and reverse tripwires. As the apparent threat to the American community and, specifically, the U.S. Ambassador has diminished, the committee agreed he no longer needs an armed DS escort with him for all moves. The RSO is drafting specific tripwires regarding a Noncombatant Evacuation Operation along with a set of reverse tripwires. The

tripwires will be presented to the EAC for discussion and approval. (Appendix source 1)

¶20. (SBU) NEA Algeria - EAC Algiers met March 29 to review the draft Memorandum of Agreement (MOA) for the security and force protection of DoD elements and personnel. The draft of the new MOA was provided to the U.S. Embassy by U.S. Africa Command. Committee members discussed the DoD presence at Post, reviewed the MOA draft, and recommended the Ambassador sign the agreement with one small correction. The Embassy will advise when the MOA is completed and signed. (Algiers 0305)

¶21. (S//NF) United Arab Emirates - On March 26, U.S. Embassy Abu Dhabi and Consulate General Dubai held a joint core EAC meeting to discuss the increase in reporting on possible United Arab Emirates (UAE) and Dubai-focused threats. The EAC members agreed, even if they lacked specific credible information, the general increase in threat-related reporting is a cause for concern. Consular officers pondered over whether it was time to discuss stronger language in the UAE Country-Specific Information. The committees agreed that, if warranted, a more focused caution be considered before the next EAC meeting. (Appendix source 2)

¶22. (SBU) EAP Taiwan - Six members of the China Patriotic Alliance arrived at the American Institute in Taiwan (AIT) on March 30. The group photographed the area, shouted slogans, and carried banners stating such things as, "Protest against U.S. meddling in the affairs of Taiwan and China." Police presence was sufficient for this event, which ended without any problems. (RSO AIT Spot Report)

¶23. (SBU) SCA Pakistan - EAC Lahore convened March 30 to discuss the attack on the police training center in Marawaan, 15 km from Lahore along the road to the Wagah border. After summarizing the attack, the principal officer suggested official Americans should refrain from any travel on the Lahore-Wagah road until the situation was resolved. A similar message will be conveyed to AmCits through a Warden Message. (See the Key Concerns section for further information on this attack.) (Lahore 0065)

¶24. (U) Key Concerns

¶25. (SBU) AF Nigeria - On March 30, DS/TIA/OSAC passed the following tearline to a named multinational company's U.S. headquarters. "Allegedly, (the named company) in Bayelsa State ran the risk of attack from the local community in the Southern Ijaw Local Government Authority due to grievances over a Memorandum of Understanding. There is no further information on the exact timing, method, or location of any attack." The company's U.S. headquarters was previously unaware of the information and was still considering options to address the situation. (DS/TIA/OSAC)

¶26. (S//NF) NEA Saudi Arabia - Recent increase in Diplomatic Quarter security: According to a sensitive source claiming firsthand access, on March 26, the Diplomatic Quarter (DQ) uniformed police disseminated an alert warning of a heightened threat to the DQ that remained in effect as of March 29. According to the alert, an unknown caller warned of an impending attack against the DQ. Three additional uniformed officers were noted at the U.S. Embassy, while two additional officers were staffed to the UK Embassy. No further information on the origin of the threat information is provided; although, on March 25, the Saudi Mabathith received an e-mail threat against the U.S. Embassy threatening an attack within the upcoming week.

¶27. (S//NF) DS/TIA/ITA also notes sensitive information, likely related to the Mabathith, warning of possible extremist activity against U.S. interests, which read, "On March 21, an unidentified person claimed that he and his associates planned to attack U.S. Embassy Riyadh. The plan involved explosives and was scheduled for the current week." The increased Saudi security posture around the DQ and Post in particular is reflective of host-nation concern for the

welfare of its diplomatic community, even if the reasons for the increased vigilance are not always made clear. (Appendix sources 3-5)

¶28. (S//NF) SCA Afghanistan - Al-Qa'ida, Taliban plans to attack embassies with toxins: As of late March, Taliban and al-Qa'ida devised a plan to conduct an attack against embassies, consulates, and offices of the U.S., Germany, France, and other countries in Kabul and other cities in-country. The Afghan National Directorate of Security (NDS) claimed Sirajuddin Haqqani, Maulawi Sadiq Agha from Kandahar Province, Maulawi Tahi from Wardak Province, and Mullah Nasar from Ghazni Province had an unspecified number of suicide bombers for the attack. Additionally, the explosives and materials for attack were toxic in some fashion. A separate type of poison, placed in an unspecified power and powdered milk, was provided to the Taliban commanders in Kabul, Wardak, Kandahar, Farah, and Helmand provinces. The poison was intended to be used in cars or residential areas of key governmental officials and could cause serious brain damage.

¶29. (S//NF) DS/TIA/ITA assesses this reporting from the NDS to be not credible. Nevertheless, multiple reports over the last year indicate al-Qa'ida, the Haqqani network, and the Taliban have focused on targeting diplomatic assets in Kabul. However, militants in Afghanistan currently lack technical abilities to produce, weaponize, and deliver toxins in warheads. While there has been some reporting of the presence of al-Qa'ida experts in chemical and biological weapons in the Afghanistan-Pakistan area who could work with the Taliban, there has been no evidence to indicate the al-Qa'ida presence in this area has effectively prepared toxins for a mass-casualty attack. That said, it may be possible to poison foodstuff to a limited effect. In early September 2008 (as well as earlier in 2008 and 2005), a pharmaceutical sedative, Lorazepam, was found in candy and almonds being distributed in Kabul. The NDS arrested an individual suspected of being a distributor for an unidentified network operating in Kabul. Consuming several of the candies possibly contained enough sedative to cause disorientation, lethargy, or unconsciousness.

¶30. (S//NF) This reporting is likely an echo or circular reporting to the following tearline from March 24.

¶31. (S//REL TO USA, NATO) "Insurgents in Afghanistan were reportedly planning in late March to carry out attacks on French, German, and U.S. political representations, embassies, and consulates in Kabul and the Afghan provinces of Wardak, Ghazni, Kandahar, Farah, and Helmand. Some of these attacks would include explosives containing an unidentified poison." (Appendix sources 6-8)

¶32. (S//REL TO USA, AUS, CAN, GBR, NZL) Kyrgyzstan/Uzbekistan - IJU cell preparing for unspecified attack: Tearline reads, "The Islamic Jihad Union (IJU) has assembled a cell of operatives in the Jalalabad area of Kyrgyzstan. Information from mid-2008 through February indicates that one of these operatives may be used for a suicide mission in an undisclosed location outside of Kyrgyzstan, possibly in Uzbekistan. Two members of the cell known as Sadiq and Ali were trained in Pakistan by the IJU in 2007 and have been charged with the safe keeping of this operative. The operative arrived in Kyrgyzstan sometime in late July or early August 2008 and has been isolated in a mountainous area nearby where he apparently still remains awaiting further instructions from the IJU leadership in Pakistan."

¶33. (S//NF) DS/TIA/ITA notes the IJU is likely seeking to conduct a high-profile attack outside of Afghanistan in order to re-establish its presence as an organization with the ability to conduct operations in Central Asia or, perhaps, Europe. While Uzbekistan remains its central target, the IJU has also threatened to carry out attacks in other locations. Some of these include the following.

¶34. (S//NF) Unverified tearline from early January 2008 states, "The IJU may be planning future terrorist operations

in Kyrgyzstan. An IJU operative in Kyrgyzstan identified as Hasan Suleymanov, who uses the alias Fara, revealed in late December 2007 that 'big works' were currently being planned for the future, presumably in Kyrgyzstan."

¶35. (S//NF) Tearline from mid-February 2008 reports, "The IJU threatened in early February to launch bloody attacks against the Government of Kazakhstan if it did not meet specific demands regarding the treatment of several members of the IJU currently on trial in Kazakhstan. A closed trial for a group of 15 people accused of plotting terrorist attacks in south Kazakhstan began in mid-January. The IJU maintained the innocence of these individuals, claiming that Kazakhstan is only used as a travel passageway by the IJU, whose real target is Uzbek President Islam Karimov and his government. The IJU apparently demanded that this group be treated humanely and not be extradited to Uzbekistan."

¶36. (S//NF) German authorities broke up an IJU cell in September 2007 believed to be targeting U.S. military interests in Germany.

¶37. (S//NF) The IJU assassinated the Kazakh deputy chief of mission to Pakistan in Islamabad, Pakistan, in January 2005.

¶38. (S//NF) Previous reporting indicates Sodiq is an IJU operative in Kyrgyzstan and may now constitute a central figure in the IJU's facilitation network there. As of January 2008, IJU facilitator Gofir Salimov (a.k.a. Jafar, Jafar the Uzbek) was attempting to re-establish contact with IJU members in Kyrgyzstan, which it appears he has done. Salimov was seeking to establish direct communication with Sodiq because he was uncomfortable communicating through an IJU member named Fara. His suspicions of Fara are probably accurate. Fara is an alias for Hasan Suleymanov, who is also known as "Bay." He was arrested by Kyrgyz authorities in February 2007 and presumably released, since he is reported to have been involved in IJU plans in December 2007. He may be working for Kyrgyz intelligence authorities. As to his current whereabouts, a tearline from mid-December 2008 reports, "Kyrgyz IJU operative Fara arrived in Panjgur, Pakistan, along with some companions in early November." It is unclear if Fara or the Kyrgyzstani Committee for National Security is aware of the IJU cell and the suicide bomber in the Jalalabad area.

¶39. (S//NF) A body of reporting in late 2007 and throughout 2008 indicates the IJU was attempting to re-establish facilitation cells in Kyrgyzstan and, more broadly, across Central Asia. However, the IJU has faced difficulty in reconstituting its operational presence in Central Asia. The crackdown on IJU activists across Central Asia since 2004 and the breakup of the IJU cell in Germany from September 2007 onward decimated its global network. Much of its operational tempo has been focused in Afghanistan, regularly working with the Haqqani network to conduct indirect and suicide attacks in southeastern Afghanistan. The IJU has also used the Internet to appeal to Central Asian and European Islamic extremists. It conducts sophisticated media operations that advertise the group's activities in Afghanistan in order to solicit funding and recruits. Despite operational failures, the IJU will continue seeking to target Uzbek and Western assets in Central Asia, primarily Uzbekistan, or wherever feasible. (Appendix sources 9-13)

¶40. (S//FGI//NF) Pakistan - March 30 attack near Lahore: Although preliminary information cited higher casualty figures, incoming reporting indicates approximately 10 gunmen armed with grenades, assault weapons, and possibly suicide vests, and some of whom wore outfits resembling police uniforms, scaled a boundary wall of the Manawan Police Training Center on March 30 and attacked unarmed police recruits conducting morning drills on the center's parade grounds. The assailants hurled grenades at recruits before opening fire and ultimately entering the center's three-story main office building, holding 35 hostages on the top floor of the compound. Pakistani security forces gained control of the compound after an 8-hour standoff punctuated with intense

firefights, resulting in the death of at least eight police officers and civilians, and the injury of more than 100. Press reports also suggest six gunmen died, and four others are in Pakistani custody. Unverified press reports suggest the gunmen shouted, "We have come, oh attackers of the Red Mosque." Pakistani police officials have described them as being Afghan. Associate Press reports note the spokesman for a group called Fedayeen Islam claimed responsibility for the attack.

¶41. (S//NF) Although details remain fluid, this latest attack underscores the continuing vulnerability of Pakistani security forces despite repeated attacks against their assets, as well as the declining security environment of the formerly tranquil Punjab Province. The use of multiple armed operatives is reminiscent of the March 3 ambush of the Sri Lankan cricket team's motorcade in Lahore; although, it remains unclear which group carried out this earlier attack. Likewise, information on Fedayeen Islam remains fragmentary, but indicates it is possibly an al-Qa'ida offshoot, if it in fact exists. Fedayeen Islam's purported spokesman also claimed responsibility for the September 20, 2008, bombing of the Marriott hotel in Islamabad, while separate intelligence reporting from mid-September and -November 2008 suggested an al-Qa'ida off-shoot group called Fedayeen (variant: Fidayeen) sought to attack U.S. Consulate Peshawar.

¶42. (S//NF) Previous attacks against Pakistani security forces training centers have almost exclusively relied upon one or two suicide operatives and have been linked to Tehreek-e-Nafaz-e-Shariat-Mohammadi, Tehrik-e-Taliban Pakistan, and al-Qa'ida. The Sunni extremist group Lashkar-e-Jhangvi has also proved capable of launching attacks in Lahore and is suspected of coordinating the December 24, 2008, truck bombing in the heavily guarded GOR-II section that killed one passerby and injured four others. Earlier attacks include the following.

- o October 9, 2008: A suspected suicide operative driving a green Suzuki four-door vehicle targeted a residential and training facility of Pakistan's Anti-Terror Force in sector H-11 of Islamabad, wounding at least seven and severely damaging the three-story building.
- o August 2, 2007: A police officer shot and killed a suicide operative wearing explosives and armed with weapons who attempted to enter a police academy in Sargodha.
- o March 30, 2007: A suicide operative disguised as a beggar killed two and injured seven at a Pakistani army training center near Kharian, Punjab Province.
- o November 8, 2006: Following a Pakistani air strike against an extremist training compound in Bajaur Agency, a suicide bomber killed 42 army recruits in Dargai, Northwest Frontier Province, while the trainees were conducting morning drills.

(Open sources; Lahore 0064; Appendix sources 14-16)

¶43. (S//NF) Pakistan - Militants planning attacks in Peshawar and tribal areas: Tearline notes, "Militants planned to target U.S. interests, Pakistani law enforcement authorities, military officials, and members of parliament in Peshawar, according to late-March Pakistani information. Also, 15 to 20 militants planned to ambush government officials traveling from Timergara to Maidan."

¶44. (S//NF) Various reports since late February suggest extremists seek to strike against U.S. and Pakistani targets in and around Peshawar by orchestrating kidnappings, assassinations, rocket attacks, or bombings. It is likely this latest report is an echo of previous information conveying these ongoing concerns. It is also possible the warning reflects reactions to Pakistani press reporting of a March 28 seizure of 120 kg of explosives, 20 hand grenades, 10 rocket propelled grenades, and explosives containers and detonators during a pre-dawn raid against a house in Shehgai Hinkian located on Warsak Road on the outskirts of Peshawar. The house allegedly belonged to Noor Mohammad, possibly a reference to Noor Mohammad (Terrorist Identities Datamart Environment number 9167174), a Haqqani network facilitator for Arabs active in eastern Afghanistan operations who is known to maintain a presence in Peshawar. Likewise, the

reference to ambush threats to officials transiting Timergara and Maidan may reference separate Pakistani press reporting from March 30 detailing a clash between police officials and the kidnapers of a bank manager in Lower Dir District, 4 km outside of Timergara, that killed five. (Appendix sources 17-28)

¶45. (U) Threats & Analysis

¶46. (S//NF) AF Nigeria - Kidnappings in the Delta: An examination of reporting and kidnapping statistics in the Niger Delta suggests kidnappings are increasingly assuming three distinct forms: militant, criminal, or political. Militant kidnappings are the greatest threat to Western expatriates, namely oil workers, while criminal kidnappings can impact both Westerners and other international oil workers. Political kidnappings tend to target local Nigerians; although, some non-Western expatriates have fallen victim to these abductions. In all these instances, the victims are usually released after monetary or political demands are met. Rarely are the victims killed; although, some have died while in custody.

¶47. (S//NF) An examination of intelligence reveals the kidnapping of expatriates peaked in 2007 with approximately 173 foreign oil workers being abducted in the nine Niger Delta states of Akwa Ibom, Bayelsa, Cross River, Delta, Edo, Rivers, Abia, Anambra, and Imo. During that same year, nine U.S. nationals were abducted. Since then, the total number of expatriate hostages has decreased. In 2008, 76 expatriates were kidnapped, with only one American kidnapped. As of early March, 13 expatriates had been kidnapped, with no Americans being abducted. The decrease can likely be attributed to better security by oil companies and the withdrawal of some oil workers.

¶48. (U) Militant kidnappings

¶49. (S//NF) Militant kidnappings probably pose the greatest threat to Western interests in the Delta region, especially due to the large density of international oil companies operating in the area. Culprits for these types of kidnappings fall under the larger group umbrella of the Movement for the Emancipation of the Niger Delta (MEND) and smaller militant organizations. Besides monetary motives such as ransoms, they may also have political motives. For example, the MEND is currently holding two British expatriate hostages. The group is hinging the hostages' release on the freedom of detained MEND leader Henry Okah.

¶50. (S//NF) A hallmark of militant kidnappings is the ability to conduct them off shore against expatriate workers on oil platforms and ships present in the Niger Delta. These types of operations are well organized and planned in advance by militants who have resources and funding. They usually involve armed men, dressed in military fatigues and riding in boats, raiding a platform or ship and kidnapping expatriate employees. Given the resources and training required for these types of kidnappings, they are normally organized by prominent militants such as Victor Ebikabowei (Boyloaf), Government Ekpemupolo (Tompolo), and Farah Dagogo.

¶51. (S//NF) One of the more brazen offshore militant kidnappings occurred on June 19, 2008, when a U.S. Citizen was briefly abducted after militants launched an attack on the Bonga Offshore Oil platform, owned by Shell Oil. While returning home, the militants boarded a ship belonging to Tidewater Marine, a U.S. company, and kidnapped its captain, Jack Stone, who worked for Chevron Oil. He was released, unharmed, within hours. To date, the Bonga attack represents the farthest offshore operation militants have conducted.

¶52. (U) Criminal kidnappings

¶53. (S//NF) Amidst the plethora of kidnappings in the Niger Delta, a criminal hostage-taking industry has also emerged. Usually, criminal kidnappings are motivated by the abject poverty afflicting the Delta region and the subsequent need

to garner cash quickly. Differentiating between criminal and militant kidnappings can be difficult, since culprits of both attacks will target international oil workers; although, Nigerians have also been victims of criminal kidnappings. Non-Western oil workers are traditionally targeted in criminal abductions; however, Western oil workers and their families have also been victims.

¶54. (SBU) Indeed, the most notorious case of criminal hostage-taking is probably the abduction of 3-year-old Margaret Hill, the daughter of a British oil worker, on July 5, 2007, as she was being driven to school in Port Harcourt, Rivers State. Although the criminals initially demanded a 5 million Naira ransom, she was allegedly released without a ransom being paid.

¶55. (S//NF) According to reporting, the victims of these abductions often practice less-stringent security protocols; hostages are abducted in traffic, in their houses, and on their way to work. Immediately after the kidnapping, the abductors usually ask for a significant ransom and rarely have political grievances that accompany many of the militant kidnappings. As such, these abductions are typically conducted by cultist groups, petty criminals, or lower-profile militants who lack the capability of more established militants.

¶56. (U) Political kidnappings

¶57. (S//NF) Political kidnappings usually target Nigerian nationals, including children and spouses of high-profile Nigerians. Culprits have conducted these types of operations against high-ranking local politicians, local businessmen, religious figures, and celebrities. Notable political kidnappings include the abduction on February 7, 2008, of Chief Olu Benson Lulu-Brigg's wife in Rivers State; the abduction of Bayelsa State Deputy Governor Perembowei Ebebi's father on December 10, 2007; and the kidnapping of former Minister of Petroleum Edmond Daukoru's wife on February 3, ¶2009.

¶58. (S//NF) The foundation for political kidnappings was created in the 2003 elections, when several politicians promised money to Niger Delta militants to intimidate the opposition. After the politicians came to power, many militants turned on them when they realized the politicians were reneging on their deals. In fact, according to one report, on September 12, 2007, a local Bayelsa State politician advised local politicians to adhere to promises to their campaign workers after police arrested three suspects in the kidnapping of 70-year-old Nigerian Laura Canus.

¶59. (S//NF) Political kidnappings may also be targeted at expatriates by local community members or disgruntled workers. In fact, on October 9, 2007, workers of the Ajakouta Steel Company kidnapped 11 Indian employees due to work condition grievances. That being said, political kidnappings remain the less immediate threat to expatriates and Westerners. (Open sources; Lagos 0222; Niger Delta Hostage Tracker; Appendix sources 29-34)

¶60. (U) Cyber Threats

¶61. (S//NF) Iran - Interest in U.S. technology and operations:

¶62. (S//NF) Key highlights:

- o Several Iranian institutions and organizations conduct OSINT against USG programs.
- o Most of the Iranian universities involved in this activity maintain longstanding ties to the IRGC.
- o Information gleaned from OSINT can be used in subsequent exploits.
- o Persistent attempts to collect U.S. information could jeopardize the security of U.S. operations and personnel.

¶63. (S//NF) Source paragraph: "Between January 21, 2007, and February 24, 2009, FACC (Farhang Azma Communication Company)

IP (Internet Protocol) addresses directly browsed a number of U.S. Navy unit websites and systematically downloaded over 100 U.S. Navy unit webpages using software 'Web Downloader/8.1.'

¶64. (S//NF) CTAD comment: According to numerous DoD reports, students and researchers at a number of prominent Iranian universities and companies have been performing open source intelligence (OSINT) collection operations targeting U.S. information for several years. OSINT is defined as "information of potential intelligence value that is based on publicly available data (e.g., academic research, databases, forums, official and draft documents, online publications, reference material, Web logs, and websites)." Persistent OSINT efforts show the continued interest and knowledge of U.S. capabilities and operations by Iranian institutions, as well as the Government of Iran (GoI). Individuals from many Iranian universities, as well as a variety of commercial organizations, also routinely attempt to solicit information from cleared defense contractors and U.S. firms via socially engineered e-mail messages in order to acquire information related to restricted U.S. operations and research. This information could then be used to develop similar programs for the GoI, shared with third-party entities (e.g., Islamic extremist groups), or exploited through additional Iranian computer network operations activities.

¶65. (S//NF) CTAD comment: Since at least January 2007, individuals using IP addresses assigned to the Internet service provider FACC have conducted extensive open source searches on information pertaining to DoD equipment, weapons systems, unmanned vehicle technologies, communications, and intelligence systems. Activity from FACC-owned IP addresses has also included searches of specific U.S. facilities in Iraq and Afghanistan, vehicles, vessels, and individual leaders. Individuals conducting these queries also used the open source software program Web Downloader in order to facilitate the simultaneous aggregation of vast amounts of data from a variety of sources. Unfortunately, the expansive time frame and scope of this activity have inhibited more precise attribution.

¶66. (S//NF) CTAD comment: As of January 2008, IP addresses within those allocated to Amirkabir University of Technology (AUT) and Malek Ashtar University of Technology (MUT) in Tehran were used to conduct OSINT operations against a number of highly sophisticated technology projects, particularly those related to unmanned aerial vehicles (UAVs) and autonomous underwater vehicles. Information and countermeasures derived from the collection and analysis of this type of information have been incorporated into AUT and MUT research programs and capabilities. In addition, the universities' research is likely provided to GoI agencies and shared with groups in other countries (see CTAD Daily Read File 09-067). DoD reporting indicates a variety of groups within AUT have maintained ties to the Iranian Revolutionary Guard Corps (IRGC) since 1998, while MUT researchers are connected to Ministry of Defense projects involving UAVs and other small aircraft.

¶67. (S//NF) CTAD comment: Since at least May 2008, OSINT searches of DoD information from IP addresses registered to Isfahan University of Technology (IUT) have also illustrated Iran's continued interest in U.S. technology. In addition to the aforementioned lists of topics targeted, IUT students have queried the environmental effects on the various technologies and budget data. Some of the IUT searches have also focused on low-cost programs and information concerning U.S. equipment produced in China and Russia, which provide Iran with a significant amount of technological data and tools.

¶68. (S//NF) CTAD comment: Although the majority of the information sought through Iranian OSINT collection efforts pertains to military capabilities and technological development, other USG departments and agencies could also become (or continue to be) targets of foreign actors' extensive online research. For example, as the U.S. pursues

increased discussions with other countries such as Iran, state-sponsored and independent actors may seek to gather information in order to hinder the success of constructive discourse or attempt to exploit individuals involved. Publicly available tools help automate the process of identifying and cataloging information for OSINT, exponentially increasing the amount of data actors can amass. However, OSINT collection is also aided by the rapidly growing quantities of information accessible to Iranian and other foreign actors, which is supplied through the aforementioned list of open source materials. Therefore, users must remain alert to and minimize the potential threats associated with the misuse of personal and professional information posted to online resources. (Appendix sources 35-39)

¶69. (U) Suspicious Activity Incidents

¶70. (SBU) EUR Armenia - A Middle Eastern-appearing male photographed his friend with U.S. Embassy Yerevan in the background March 22. The subjects arrived in a vehicle with Iranian license plates. Police stopped and questioned the men, who claimed to be tourists interested in the Ararat Mount view. A check of the camera showed no photos of Post. The subjects drove away right after the interview.

¶71. (SBU) RSO Action/Assessment: The RSO provided the following assessment of recent Iranian activity in Yerevan on March 30. "Several incidents involving Iranians and Iranian families have been observed in the past two weeks in Yerevan. While surveillance events in a large part are seasonal, coinciding with warmer weather and summer holidays, several factors have existed to explain in part the sudden rise in Iranian activity near and around the Embassy. Yerevan recently hosted an Iranian musical troupe that overlapped with the traditional Iranian New Year holiday of Nowruz. Both events saw a significant increase in Iranian tourists in Yerevan, which very well may have been the cause of increased Iranian activity. Secondly, the Embassy is located on a main (and only) thoroughfare from both the airport and southern access of Armenia and Iran. The Embassy is also adjacent to a favorite tourist location, the Admiral Isakov Monument. Although most if not all Iranians are not familiar with this World War II Soviet-Armenian war hero, it is a noticeable statue adjacent to Post that affords an excellent view of Mt. Ararat. All Iranians challenged by the Surveillance Detection Team (SDT) were cooperative and non-combative, unlike many European tourists. Nonetheless, all incidents involving Iranians are closely monitored by the RSO. No further action required at this time." (SIMAS Event: Yerevan-00645-2009)

¶72. (SBU) The Netherlands - A man stood by the back gate of U.S. Embassy The Hague March 25. The subject had two black bags with him and played with his cell phone while occasionally looking at the back gate. After 20 minutes, the guard from the French Embassy located across the street from Post told the subject to leave the area, which he did. (SIMAS Event: The Hague-00861-2009)

¶73. (SBU) Ukraine - A man in a white truck pulled up near U.S. Embassy Kyiv on March 26. The subject photographed the surrounding area with a cell phone camera. LGF and National Guard members stopped and questioned the man, who indicated he transported someone to a beauty shop located nearby; however, the LGF noticed that he arrived in the area alone. He also said he was "testing his cell phone camera" and erased the images before the guards arrived. After showing some identification, he departed the area.

¶74. (SBU) RSO Action/Assessment: Because of the inconsistency in his story, the RSO requested police conduct records checks and investigate the subject. As more information becomes available, it will be reported.

¶75. (SBU) Record Check/Investigation: Subject: Olexander Mykolaiovych Levchenko. Identification number: KIA 222385; Issue date: November 16, 1999 (Kyiv). (SIMAS Event: Kyiv-00638-2009)

¶76. (SBU) AF Ghana - Two men stood at a bus stop in Accra on March 25 photographing each other with the U.S. Ambassador's residence in the background. The police were notified, and they stopped and questioned the subjects. Police erased the photographs, cautioned the men against photographing USG facilities, and allowed them to leave.

¶77. (SBU) Record Check/Investigation: Subject 1: N'Dimbi Biyenga. Cell phone number: 0245425491. Identification number: 236408. (SIMAS Event: Accra-01185-2009)

¶78. (SBU) NEA Bahrain - A man (later identified as a Yemeni citizen) parked his vehicle near U.S. Embassy Manama March 29. After an hour, the subject got out of his car, walked around the area, and then departed.

¶79. (SBU) Record Check/Investigation: A police license plate check lists the owner of the vehicle as Mas'ad Ali Mohammed Alward. Bahraini identification number: 61042046. The subject lives in a neighborhood close to Post. The SDT will be on the lookout for this man. Details of the incident were also passed to the Naval Support Activity, Bahrain Threat Mitigation Group. (SIMAS Event: Manama-00146-2009)

¶80. (SBU) Jordan - A suspicious vehicle parked near U.S. Embassy Amman on March 29. The driver looked around the area for 20 minutes. He then moved and parked the car 30 meters from the back gate of Post. LGF members and police checked the vehicle with negative results. The driver was not in the vehicle (NFI). (SIMAS Event: Amman-03604-2009)

SECRET//FGI//NOFORN//MR

Full Appendix with sourcing available upon request.
CLINTON